GSMA Position Paper for Web Cryptography Next Steps Workshop Hardware Tokens: SIM Applets for use in Mobile Connect 28/07/2014

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

GSMA Position Paper for Web Cryptography Next Steps Workshop

Hardware Tokens: SIM Applets for use in Mobile Connect

This Document

This document details the "Position Paper" for the "Web Cryptography Next Steps Workshop"[1] organised by the W3C. The event takes place on 10-11 September in Silicon Valley.

Introduction

The GSMA[2] represents the interests of mobile operators worldwide and connects them with companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. Collaboratively with our members the GSMA runs a number of technical programs and interest groups; among these is the Personal Data programme, the Digital Commerce Programme and the Web Working Group.

The Personal Data[3] programme aims to develop a set of digital identity services for mobile subscribers. GSMA and it's member operators are working together to bring identity solutions which prioritise customer experience, security and low barriers to entry.

The Digital Commerce[4] programme works with operators and vendors to build new mobile

[1] http://www.w3.org/2012/webcrypto/webcrypto-next-workshop/
[2] http://www.gsma.com/aboutus/
[3] http://www.gsma.com/personaldata/
[4] http://www.gsma.com/digitalcommerce/

payment and transaction technologies using mobile wallets and NFC functionality throughout industries such as retail, transport and personal finance.

The Web Working Group is in charge of monitoring activity in the web landscape and identifying these programmes of opportunities for operators within the web. The group also manages standards body engagement, working with both the W3C, IETF and 3GPP.

This paper will focus on the identity solutions being developed within the Personal Data programme, and the use of hardware tokens as a security feature within these solutions.

Personal Data Programme

The GSMA's Personal Data programme is working with operators and service provides to create a set of solutions which include authentication, identity, attribute validation, and attribute brokerage; these are collectively referred to as "Mobile Connect"[5]. These solutions will allow consumers to gain access to digital services and/or use their mobile device for authentication at different levels of assurance. Developers and service providers will be able to use Mobile Connect to allow their users to login, access services and prove their identity safely and securely.

Mobile Connect is based on the OpenID Connect[6] protocol. It uses the user's mobile phone number in the similar way to a "username"; this is used together with information stored securely within the users SIM card to allow the user access to services or to provide proof of their identity.

An Example Flow: Mobile Connect Two Factor Authentication

"Mobile Connect" offers four levels of identity assurance; the first level allows a user to simply login to a website or application with added security by using two-factor authentication. The user will visit the application (on their mobile device or desktop) and see a "Mobile Connect" button, once they click the button the application will ask the user to "check their mobile phone". The user's mobile device will then display a notice asking the user whether they wish to allow access to the application; if they click "yes" they gain access. Given the user's mobile device is usually in their possession they can be assured that a third party can only gain access to their account on an application when that third party has both their login details and their mobile device.

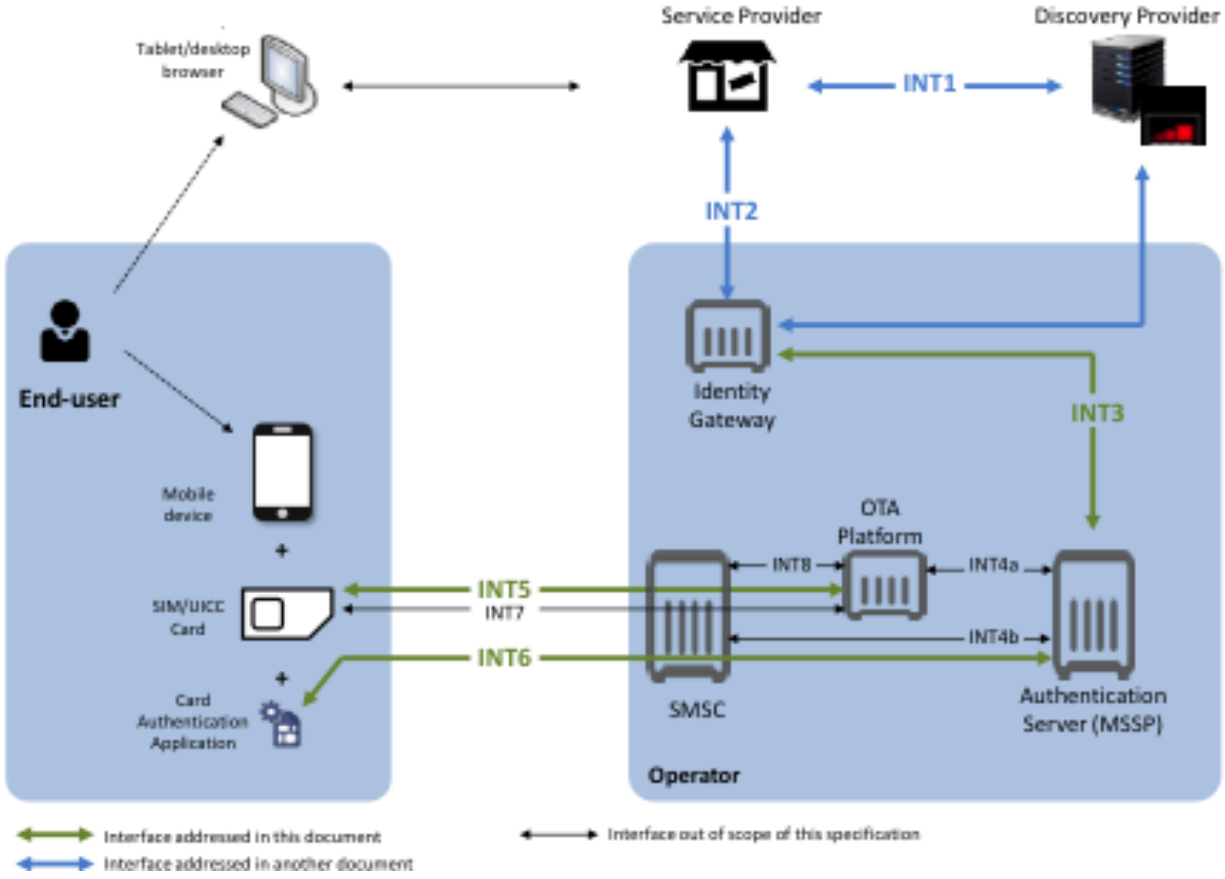
Use of the SIM as a Hardware Token: SIM Applet

For a selection of "Mobile Connect" services newly developed SIM cards (UICC[7]) are used which hold a CPU, ROM, RAM, EEPROM and I/O circuits[8] which allow small programs (or "applets") to be stored and run directly from the SIM. An applet's size is dependant on the UICC card being used together with the operating system used to configure it; a 32kb Java Card[9] can

[5] http://gsmamobileeconomy.com/gsmamc/
[6] http://openid.net/connect/
[7] http://en.wikipedia.org/wiki/Universal_Integrated_Circuit_Card
[8] http://www.etsi.org/deliver/etsi_ts/102200_102299/102241/11.00.00_60/ts_102241v110000p.pdf
[9] http://en.wikipedia.org/wiki/Java_Card

usually hold an applet of around 32kb. The benefits of running applets on the SIM are detailed in "SIM Applets: Benefits and Drawbacks".

In Mobile Connect the applet loaded and run from the SIM manages authentication; in the below diagram it is labelled as the "Card Authentication Application". The Card Authentication Application holds one or many Authentication Handlers (authentication methods) that are installed and configured on-board of the Card Authentication Applet and that the Authentication Server can invoke to authenticate the end-user. Implementations could include one or more of: AES-CMAC, 3DES-CBC, OATH-HOTP/OCRA or PKI. The below diagram also shows the division between technologies on the device and technologies within the operator domain, and those working outside.



SIM Applets: Benefits and Drawbacks

The benefits of running small applets from the SIM are security based:

- A single factor of authentication: an attacker needs to have possession of the user's device and the passcode (when a passcode is in use) in order to authenticate or authorise a transaction on their behalf.
- By using the user's device in the authentication loop any unauthorised attempts to access their online account will result in them receiving an authentication request on

their device hence a clear notification that someone is trying to access their account (the user can then take appropriate action).
- Limited number of parties have access to write or read from the SIM.

One disadvantage of using the SIM is it traditionally requires applets to be written at the point of manufacture; with new "Over the Air" (OTA) architecture the programme can be written to the SIM remotely. Another drawback is the size of the SIM applet: any cryptographic method, authentication program or encryption algorithm must be small enough to fit onto the hardware token.

Future

The “Mobile Connect” use of the SIM is an example of a hardware token use and the benefits hardware tokens can bring for privacy and security. Below is a collection of ideas of how this work can be developed and standardised to widen the use of hardware tokens across the web and other technologies.

Secure Storage

PIN and other password storage is a large problem; and one which Mobile Connect is trying to solve. Some current solutions offer encrypted storage in the cloud but another offering could be hardware storage on the device. Users will then know and understand their passwords are stored, with them, on a device which is only governed by the laws within their country. An API or some defined interface to allow applications to securely access some dedicated storage area on the SIM may therefore be useful.

Secure Processing

As well as secure storage the SIM can also be used for secure processing; a cryptographic processor can be used to support high security algorithms (such as RSA 2048bit keys or Elliptic Curve Cryptography) allowing dedicated cryptographic processing away from the standard processing of a machine.

Cryptography on the SIM

As detailed above in Mobile Connect authentication can be managed with a number of different cryptographic implementations and a dedicated purpose-built API. This innovation is currently not completely standardised which can delay the uptake of the using the SIM as a hardware token for this cryptographic storage and processing as developers and service providers find the overhead of adopting this new technology is too great. A standardised method of supporting cryptography on the SIM could be developed together with an API for accessing and using cryptographic keys, secrets or credentials (etc.). Global Platform have standardised storing of these cryptographic details on the SIM[10] but a standard API has not yet been developed.

Assuring Security Prior to Issuing a Token

There is scope for some developments in further security prior to issuing a token from a user’s device. These questions are more focused on the interaction between the device, operating

[10] http://www.globalplatform.org/specificationscard.asp

system and SIM but may have impact on a web implementation of hardware token cryptography. The key questions are:

- What process and strategy should be used to authenticate a subscriber before a token is issued to a device?
- What checks can be completed to ensure the device is 'safe' prior to the token being downloaded (e.g., has it been jailbroken)?
- Is the user in control of the device, does the device need to be unlocked to receive tokens or does the user or system specifically request these tokens?

Use cases and typical scenarios should be documented to understand some of the further issues in working with hardware tokens.

Final Remarks and Opportunities for the Web

This document has showcased the Mobile Connect solution and it's use of the SIM as a cryptographic hardware token to improve security for users when interacting with web and other online services. Mobile Connect makes use of UICC (new SIM cards) to create an authentication applet which can hold various cryptographic methods. The benefits of these were shown to offer users increased peace-of-mind and security as they both know the method of access to their accounts is always in their possession (through their device). After this we documented some proposed future developments: greater standardisation in storage and APIs to access hardware token functionality including storage of important data and cryptographic processing. Although only lightly touched on we detailed some key security and device-flow questions which will need to be answered in the development of new interfaces to hardware tokens which were proposed above. GSMA will happily bring it's experiences with Mobile Connect and suggestions for developing the use and interfaces to hardware tokens to the W3C Web Cryptography Next Steps Workshop.